PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-091427

(43)Date of publication of application : 10.04.1998

(51)Int.Cl. G06F 9/06
G06F 12/14

(21)Application number : 09-151747

(22)Date of filing : 10.06.1997

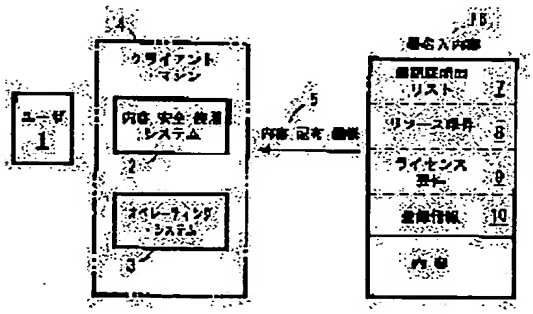
(71)Applicant : INTERNATL BUSINESS MACH CORP <IBM>

(72)Inventor : ANAND RANGACHARI
ISLAM NAYEEM
RAO JOSYULA RAMACHANDRA

(30)Priority

Priority number : 96 661687 Priority date : 11.06.1996 Priority country : US

(54) METHOD AND SYSTEM FOR GUARANTEEING SAFETY IN USING CONTENTS WITH SIGNATURE



(57)Abstract:

PROBLEM TO BE SOLVED: To safely execute a software from an unreliable source by providing an analyzing module which is an extracting device extracting a signature part from contents with a signature and executing correction when a doubt exists in reliability and safety and a reinforcing module which guarantees that a usage of contents with a signature coincides with a resource important matter and an admission certification.

SOLUTION: A user 1 uses a client machine 4 and uses content distributing mechanism 5 for transferring the contents 6 with the signature to its machine. The contents is provided with the signature, the signature has four blands and the first blank 7 is the list of a software admission certification. The contents with the signature is down-loaded by a content importing system. The extracting device analyzes the blanks of the signature and gives the information to the analyzing module. The analyzing module recognizes safety, investigates the list of the admission certification in security and decides a reliability level. The analyzing module investigates and decides the resource important matter so as to give the information to the reinforcing module.

CLAIMS

[Claim(s)]

[Claim 1] It connects so that the contents with a signature imported according to the contents import device and the above-mentioned import device may be received. The above-mentioned extractor which is an extractor which extracts the part of a signature from the above-mentioned contents with a signature, and includes the requirements for a resource for the above-mentioned part to use the approval certification and the above-mentioned contents relevant to the above-mentioned contents, When [which the above-mentioned extractor supplied] the dependability and integrity of contents with a signature are checked at least using approval certification and misgiving is in any of dependability and integrity they are The contents insurance use system used in the computer system characterized by having the analysis module which takes amendment actuation, and the strengthening module which guarantees that use of contents with a signature is in agreement with the requirements for a resource, and approval certification.

[Claim 2] The above-mentioned extractor is a system according to claim 1 characterized by having further a means to extract registration information from a signature, and having further a means to register contents with a signature into a provider, without interfering with a user further.

[Claim 3] It is the system according to claim 1 which the above-mentioned extractor has further a means to extract license conditions from a signature, and is characterized by guaranteeing that the above-mentioned strengthening module's performing an operating system and a dialogue and using these contents corresponds with license conditions.

[Claim 4] It is the system according to claim 1 carry out having further the DS stored in the memory of the above-mentioned computer system, and the above-mentioned DS having the table showing correspondence between a user, approval certification, and the function of contents with a signature, and having a means strengthen this use when the above-mentioned strengthening module is connected so that a correspondence table may be read from DS, and a user uses contents with a signature according to the above-mentioned correspondence as the description.

[Claim 5] The above-mentioned strengthening module is a system according to claim 1 characterized by having a means to guarantee that pursue the process generated from contents with a signature, and actuation of this process is in agreement with the requirements for a resource, and approval certification.

[Claim 6] The above-mentioned import device is a system according to claim 1 characterized by being the communication channel connected to the communication network.

[Claim 7] The above-mentioned import device is a system according to claim 1 characterized by being rotation storage.

[Claim 8] The above-mentioned import device is a system according to claim 1 characterized by being the memory card in which desorption is possible.

[Claim 9] It is the system according to claim 1 which has further the DS stored in the memory of the

above-mentioned computer system, and is characterized by the above-mentioned DS having the table showing correspondence between the limits of one of the resources which the actual resource and the above-mentioned computer system which contents with a signature, the requirements for a resource, and contents with a signature consumed imposed on contents with a signature.

[Claim 10] The above-mentioned table is a system according to claim 9 characterized by license conditions including further the constraint on the use imposed on contents with a signature.

[Claim 11] It is the memory which can read the computer which installed contents with a signature. The above-mentioned contents with a signature include the contents which can read the signature which can read a computer, and a computer. The signature which can read the above-mentioned computer in order to use the contents which can read the approval certification column and computer which are contained in the distribution chain of the contents which can read the above-mentioned computer, and which include code discernment of sending agency equipment and repeating installation at least It has two or more columns containing the requirements column for a resource which identifies a required computing resource.

[Claim 12] It connects so that the contents with a signature imported according to the contents import device and the above-mentioned import device may be received. The above-mentioned extractor which is an extractor which extracts the part of a signature from the above-mentioned contents with a signature, and includes the license conditions [the above-mentioned part] which can read the computer relevant to the above-mentioned contents, The contents use system used in the computer system characterized by having the strengthening module which controls actuation of the above-mentioned computer system to guarantee that use of contents with a signature is in agreement with license conditions.

[Claim 13] The above-mentioned extractor is a system according to claim 1 characterized by having further a means to extract registration information from a signature, and having further a means to register contents with a signature into a provider, without interfering with a user further.

[Claim 14] They are the step which imports contents with a signature into computer system, and the step which extracts the part of a signature from contents with a signature. The above-mentioned step including the requirements for a resource for the above-mentioned part to use the approval certification and the above-mentioned contents relevant to the above-mentioned contents, The step which takes amendment actuation when the dependability and integrity of contents with a signature are checked at least using approval certification and misgiving is in any of dependability and integrity they are, The step which controls the operating system of the above-mentioned computer system to guarantee that use of contents with a signature does not exceed the requirements for a resource, and approval certification, How to guarantee the insurance of use of the contents with a signature in the above-mentioned computer system characterized by ****(ing).

[Claim 15] The approach according to claim 14 characterized by having further the step registered into a provider by the communication channel, without extracting registration information from a signature and interfering in contents with a signature further at a user.

[Claim 16] The approach according to claim 14 characterized by having further the step which controls the above-mentioned operating system to guarantee that extract license conditions from a signature and contents with a signature are in agreement with license conditions.

[Claim 17] The approach according to claim 14 characterized by having further the step which forms the DS containing the table showing correspondence between the certification of a user and approval, and the function of contents with a signature in the memory of the above-mentioned computer system, and the step which strengthens this use when a user uses contents with a signature according to the above-mentioned correspondence.

[Claim 18] The approach according to claim 14 characterized by having further the step which operates the above-mentioned process compulsorily so that it may be in agreement with the step and the requirements for a resource which pursue the process generated from contents with a signature, and approval certification.

[Claim 19] The contents with a signature are approaches according to claim 14 characterized by having at least one of an application program and documents.

[Claim 20] How to control use of the contents in the above-mentioned computer system characterized by to have the step which imports into computer system contents including the license conditions which can read a computer, the step which extract the license conditions which can read a computer from the contents which imported, and the step which control actuation of the above-mentioned computer system to guarantee that use of contents with a signature is in agreement with license conditions.

[Claim 21] The approach according to claim 20 characterized by having further the step automatically registered into a provider by the communication channel, without extracting registration information from a signature and interfering in contents with a signature further at a user.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the security device of the computer for performing safely software which came to hand with the means of a network or others from the unreliable source.

[0002]

[Description of the Prior Art] Since the usefulness of the computer connected by network is increased, it searches for the approach of making it possible to execute the program which these computers received from the server. The main advantages of such a system at the time of seeing from a user are that the amount of the software which must be stored in a user's computer decreases by this. Although this system has many advantages when it sees from the developer of

software, main advantages are that the provider of application can control more to distribution of a program. Use of the Java applet (namely, program) embedded on the document of World Wide Web is an example which such a system is large and has spread.

[0003] The software acquired from the server means improper use, and the important concerns to such approach damage a user's computer, or will steal [hear / I / **********] data, and there are. Therefore, the downloaded software must give only the resource of the system which these need, and the thing beyond it must be performed by the controlled environment which is not given. The main troubles of the security device of the Java applet used now are that this does not have sufficient flexibility. Java applets are considered [no] to be hostile things, and accessing the resource of most on the operating system of a user's machine is allowed.

[0004] Various things exist in the standard technique for authentication by the public key cryptosystem. RSA is an example of the public-key-encryption algorithm currently used broadly. RSAref and PGP are contained in the example of activation of this.

[0005] The device which creates a digital signature to a message exists again. These signatures connect the contents of the message to people. These can be used again, in order to create a digital signature to a message so that the implementer of a message cannot avoid responsibility for this message. The MD5 algorithm combined with RSA is an example of a signature system.

[0006] The capacity for controlling access to the resource of a system is being used for many computer operating systems. One capacity is authorization holding a process, in order to perform a certain action to other objects. There are Amoeba and Mach in the prominent operating system which is using the capacity for strengthening security.

[0007]

[Problem(s) to be Solved by the Invention] Therefore, the purpose of this invention is offering the security device for performing safely software which came to hand on a network or other means from the unreliable source.

[0008]

[Means for Solving the Problem] According to the 1st aspect of affairs of this invention, the contents insurance use system and approach of using it in computer system are offered. This system is connected so that the contents with a signature imported according to the contents import device and the above-mentioned import device may be received. The above-mentioned extractor with which it is the extractor which extracts the part of a signature from the above-mentioned contents with a signature, and the above-mentioned part includes the approval certification relevant to the above-mentioned contents, The requirements for a resource which use the above-mentioned contents, and the analysis module which takes amendment actuation when [which the above-mentioned extractor supplied] the dependability and integrity of contents with a signature are checked at least using approval certification and misgiving is in any of dependability and integrity they are, It has the strengthening module which guarantees that use of contents with a signature is in agreement with the requirements for a resource, and approval certification.

[0009] According to the 2nd aspect of affairs of this invention, the memory which can read the

computer which installed contents with a signature is offered. These contents with a signature have two or more columns containing the requirements column for a resource which identifies an operation resource required in order that the signature which can read a computer may use the contents which can read the approval certification column and the computer which are contained in the distribution chain of the contents which can read a computer, and which include code discernment of sending agency equipment and repeating installation at least including the contents which can read the signature which can read a computer, and a computer.

[0010] According to the 2nd aspect of affairs of this invention, the contents use system and approach of strengthening license conditions within computer system are offered. This system is connected so that the contents with a signature which imported according to a contents import device and the above-mentioned import device receive, it is the extractor which extracts the part of a signature from the above-mentioned contents with a signature, and an above-mentioned part has an above-mentioned extractor including the license conditions which can read the computer relevant to the above-mentioned contents, and the strengthening module control actuation of the above-mentioned computer system to guarantee that it is in agreement to license conditions in use of contents with a signature.

[0011]

[Embodiment of the Invention] The example of this invention is explained to a detail with reference to drawing. Drawing 1 summarizes and explains this invention. A user 1 uses the contents distribution device 5 for using a client machine 4 and transmitting the contents 6 with a signature to the machine. A floppy disk, CD-ROM, and the Internet are contained in the example of this distribution device. A Java applet, OLE KOMPONENTSU, and SOM KOMPONENTSU are contained in the example of the contents which can be performed. These contents have the signature. The contents of other classes can include a text, voice, and an image. A signature has four columns and the 1st column 7 is a list of approval certification of software. Drawing 3 explains this to a detail further. Discernment of the author and a manufacturer is included in the example of approval certification. These certification guarantees that the certification is created and distributed by him who is indicated by the list. Furthermore, these certification offers a means to confirm that modification is not added to these contents, after signing the contents. Furthermore, these certification offers further a means to guarantee that the author cannot avoid responsibility for the created contents. The 2nd column 8 has described the computing resource 3 which the contents need on the machine of a client. These resources are needed in order that these contents may attain that purpose on a client machine. Install and activation of contents with a signature are included in the example of this purpose. Access, RAM and CPU, and the capacity and the user display of a network to the tooth space of a disk, the tooth space of a file, and a file are included in the example of a computing resource.

[0012] If contents with a signature are downloaded in a user's machine, a user can use these contents by various approaches. Performing installing this, viewing this, and this is included in the example which uses these contents. These contents are used in the environment carefully controlled

on the machine of a client. In order to use contents with a signature in this way, it is necessary to access an operation resource on the machine of a client. A resource required in order to use the contents 8 with a signature is a part of signature of the contents. Access to such a resource is arbitrated by the contents insurance use system 2.

[0013] The 3rd column (this is an option) offers the license information 9. A service condition like the number of the machines which can use the contents, and a period is included in the example of license information. The 4th column (this is an option) is the registration information 10. This information is used in order to register the contents into a provider automatically. Drawing 2 shows an example of a contents distribution device. These contents occur on the machines 15 and 16 of a manufacturer or the author, and 17, and before downloading in the machine 11 of a client, they go via many middle machines 12, 13, and 14.

[0014] Drawing 3 shows the certification accumulated in these contents with a signature according to contents with a signature being distributed to a user's machine 20 from a manufacturer's machine 22. A manufacturer attaches approval certification to these contents, before transmitting the contents 25 with a signature to repeating installation 21 with a certain means 27. Next, this repeating installation attaches that approval certification to these contents with a signature, before transmitting the contents 24 with a signature to the next repeating installation in a distribution chain. If contents with a signature finally reach a user by such approach, this includes the list of approval certification of all repeating installation and manufacturers 23.

[0015] Drawing 4 shows the process which downloads contents with a signature from the provider 31 of the contents within the contents insurance use system 31, and the process following this. This contents insurance use system 31 is IBM. PC personal computer, IBM It can carry out as a part of general purpose computer system (not shown) like which workstation of the others suitable for using it as a RS/6000 workstation or a system of a client. These contents with a signature are downloaded by the contents import system 33. An extractor 34 analyzes the column of a signature and hands over this information to the analysis module 35. This analysis module checks the integrity of the contents. Next, this analysis module considers the list of approval certification of security, and judges access in the case of using these contents by that machine, and the level of dependability. Next, if this analysis module examines the requirements for a resource of these contents and can do them, it will judge whether these requirements can be satisfied by a user's input. Next, this information is handed over to contents interpretation equipment 36 and the strengthening module 37.

[0016] The contents import device 33 is a network interface (for example, a user is connectable with the Internet with this), a diskette subsystem, and CD. It can carry out as a ROM subsystem or a cartridge storage subsystem. An extractor 34, the analysis module 35, and contents interpretation equipment 36 and the strengthening module 37 can be carried out as a program code which can be performed by workstation which performs safe contents. As for a strengthening module, it is desirable to connect with the operating system (for it to be (like OS/2, UNIX, or Windows NT)) of a workstation. Contents interpretation equipment 36 can be carried out as a module in an operating

system, or can be made separate from an operating system like a Java interpreter program.

[0017] Drawing 9 is a flow chart corresponding to actuation of the system of drawing 4 . Contents interpretation equipment is a device which uses the contents. The Internet browser and a Java virtual machine are contained in the example of contents interpretation equipment. A strengthening module uses the level of the dependability which the analysis module judged, and creates an item in an access information table. Drawing 5 explains this table.

[0018] In order to use contents with a signature, generally it is necessary to access the resource of an operating system. Drawing 5 shows the table 40 which a strengthening module uses, in order to pursue the resource which is the contents with a signature currently used on that machine and which these contents consumed, or it required. A strengthening module uses the approval certification 41 about the contents with a signature, and judges the limit of a resource 42 where these contents with a signature should be given on the machine of a client. This judgment can be performed by various approaches including the demand of a clear input to the user for judging access which the prior configuration and the prior contents on a table should obtain. It is efficient that a strengthening module creates the capacity reflecting "who accesses what [how many]" for contents with a signature. Generally, the resource which contents with a signature obtain is the subset of the resource which a user accesses on the machine of a client. A security manager pursues the resource 43 consumed according to the contents. This is attained by guaranteeing that all accesses to the resource of the system by contents with a signature pass a security manager. This table includes the item over the resource 43 which contents with a signature required again. If the consumed resource 43 exceeds the limit 42 of a resource, or the demanded resource 44 at which time, a security manager can take amendment action. The inquiry to termination of use of contents with a signature and the user of the guidance about how it goes on is included in the example of amendment action.

[0019] Drawing 6 shows the relation between the capacity of various items. A user's privilege 51 is the subset of the privilege of an operating system 50. The contents with a signature are performed within the environment where the privilege 52 is the subset of a user's privilege. Next, the privilege of the contents 53 with a signature is the subset of the execution environment. Other contents can be used on the machine of a client by using contents with a signature. For example, the contents in which other activation is possible are installable in the process on the machine of a client by performing a Java applet. Thus, the privilege of the generated contents 54 is the subset of the privilege which was in agreement with contents with a signature. I want to care about that the effective device for fulfilling these constraint is given to a security manager by including the requirements for a resource in the signature of contents with a signature. These generated contents can be performed as long as the resource which this consumes is the limit of the resource imposed on contents with a signature. The whole of this information can be pursued within the table of the security manager who shows drawing 5 .

[0020] If contents with a signature are downloaded in a user's machine, a user will acquire the capacity which uses these contents. This capacity is connected with the user who started the

transfer. This user allows other users to use these contents with a signature by that machine. Drawing 7 shows the relation between the privilege of other users like 61, 62, and 63, and a user's 27 privilege currently installed. For example, it will be reflected in the ability of this document to be changed [whether this user can read this document, a user's privilege can be written in this document, or] if contents with a signature are the documents of Lotus.

[0021] Drawing 8 shows the example which is Java applet 80 which contents with a signature signed. The approval certification 79 on this applet is the approval certification of that author, a manufacturer, and a retailer. This applet exists on the machine 77 of a server, and is managed according to the process 78 of a server. The machine of a server and the process of a server are mere distribution devices, and it is necessary to care about that these do not need to have any relation with the author. A contents distribution device is the Internet 76.

[0022] The agent 72 of the client which acts for a user 71 and exists on the machine 70 of a client downloads an applet by contacting the process of a server. The agent of this client sends that approval certification like discernment (that public key or certification) of a user, or discernment (IP address etc.) of the machine of a client to the process of a server. A server process uses this information, proves that a user can trust it, and pursues use of an applet. Answering this, the process of a server returns the public key (or certification) of discernment of the machine of an applet with a signature, and a server, and the process of this server to a client. A server must encipher the response with a user's public key, and it must guarantee that an applet is conveyed by the machine of a client at insurance.

[0023] The agent of a client checks the integrity of the contents, and a related signature. If this is performed, the agent of a client will judge the requirements for a resource of the certification of approval, and contents with a signature. This agent decodes the response of a server using that secrecy decode key, and extracts the security information in a response (it is (like a public key or certification)), i.e., discernment of an implementer, and discernment (it is (like a public key or certification)) of the process of a server and discernment (it is (like an IP address)) of the machine of a server. This information is supplied [user / the identifier of an applet, the requirements for a resource described in the signature, and] to security strengthening equipment 74 with discernment of the machine of a client. The approval certification of the signed applet is stored as capacity constituted by TORIPURU constituted by the identifier of contents with a signature, and the requirements for a resource described [which were described and were approval-proved], and is given to a security manager.

[0024] Security strengthening equipment is similar to the security manager in the environment of time amount where Java is operating. It is a system service with the reliance which cannot be changed. This calculates the capacity that an applet can be performed on the machine of a client using the approval certification of contents with a signature. A set of contents with a signature on activation amends all calls to the resource of a system through a security manager. This security manager uses the capacity relevant to an applet, and judges whether the resource which the applet required is permitted (drawing 10). This manager can be used in order to program the range of the

policy of security, and it can opt for access which an applet with a signature has to the resource of a system. Access is clearly permitted by promoting a user with a dialog box starting with an easy policy like access that the range of this policy has no access, and perfect, and access which the user constituted beforehand.

[0025] The user who downloads an applet judges whom [other] access to this is permitted. Special capacity is made to each user. When the contents perform this, these contents perform this by the subset of a call person's access privilege. As for a security manager, the capacity given to the user of an applet can be canceled at any times.

[0026] Although the suitable example explained this invention, this contractor can make various modification and improvements. Therefore, he has to understand that this suitable example is not what is offered as one example and means limitation. The range of this invention is clarified by the above-mentioned claim.

[0027] As a conclusion, the following matters are indicated about the configuration of this invention.

(1) It connects so that the contents with a signature imported according to the contents import device and the above-mentioned import device may be received. The above-mentioned extractor which is an extractor which extracts the part of a signature from the above-mentioned contents with a signature, and includes the requirements for a resource for the above-mentioned part to use the approval certification and the above-mentioned contents relevant to the above-mentioned contents, When [which the above-mentioned extractor supplied] the dependability and integrity of contents with a signature are checked at least using approval certification and misgiving is in any of dependability and integrity they are The contents insurance use system used in the computer system characterized by having the analysis module which takes amendment actuation, and the strengthening module which guarantees that use of contents with a signature is in agreement with the requirements for a resource, and approval certification.

(2) The above-mentioned extractor is the system of the above-mentioned (1) publication characterized by having further a means to extract registration information from a signature, and having further a means to register contents with a signature into a provider, without interfering with a user further.

(3) It is the system of the above-mentioned (1) publication which the above-mentioned extractor has further a means to extract license conditions from a signature, and is characterized by guaranteeing that the above-mentioned strengthening module's performing an operating system and a dialogue and using these contents corresponds with license conditions.

(4) the above -- computer system -- memory -- having stored -- DS -- further -- having -- the above -- DS -- a user -- approval -- certification -- and -- a signature -- entering -- the contents -- a function -- between -- correspondence -- being shown -- a table -- having -- the above -- strengthening -- a module -- DS -- from -- correspondence -- a table -- reading -- as -- connecting -- having -- the above -- correspondence -- following -- a user -- a signature -- entering -- the contents -- using it -- a case -- this -- use -- strengthening -- a means -- having -- things -- the description -- ** -- carrying out -- the above -- (-- one --) -- a publication -- a system .

(5) The above-mentioned strengthening module is the system of the above-mentioned (1) publication characterized by having a means to guarantee that pursue the process generated from contents with a signature, and actuation of this process is in agreement with the requirements for a resource, and approval certification.
(6) The above-mentioned import device is the system of the above-mentioned (1) publication characterized by being the communication channel connected to the communication network.
(7) The above-mentioned import device is the system of the above-mentioned (1) publication characterized by being rotation storage.
(8) The above-mentioned import device is the system of the above-mentioned (1) publication characterized by being the memory card in which desorption is possible.
(9) ****** -- computer system -- memory -- having stored -- DS -- further -- having -- the above -- DS -- a signature -- entering -- contents -- a resource -- requirements -- a signature -- entering -- the contents -- having consumed -- being actual -- a resource -- and -- the above -- computer system -- a signature -- entering -- the contents -- having imposed -- either -- a resource -- a limit -- between -- correspondence -- being shown -- a table -- having -- things -- the description -- ** -- carrying out -- the above -- (-- one --) -- a publication -- a system .
(10) The above-mentioned table is the system of the above-mentioned (9) publication characterized by license conditions including further the constraint on the use imposed on contents with a signature.
(11) It is the memory which can read the computer which installed contents with a signature. The above-mentioned contents with a signature include the contents which can read the signature which can read a computer, and a computer. The signature which can read the above-mentioned computer in order to use the contents which can read the approval certification column and computer which are contained in the distribution chain of the contents which can read the above-mentioned computer, and which include code discernment of sending agency equipment and repeating installation at least It has two or more columns containing the requirements column for a resource which identifies a required computing resource.
(12) It connects so that the contents with a signature imported according to the contents import device and the above-mentioned import device may be received. The above-mentioned extractor which is an extractor which extracts the part of a signature from the above-mentioned contents with a signature, and includes the license conditions [the above-mentioned part] which can read the computer relevant to the above-mentioned contents, The contents use system used in the computer system characterized by having the strengthening module which controls actuation of the above-mentioned computer system to guarantee that use of contents with a signature is in agreement with license conditions.
(13) The above-mentioned extractor is the system of the above-mentioned (1) publication characterized by having further a means to extract registration information from a signature, and having further a means to register contents with a signature into a provider, without interfering with a user further.

(14) The step which imports contents with a signature into computer system, The above-mentioned step which is a step which extracts the part of a signature from contents with a signature, and includes the requirements for a resource for the above-mentioned part to use the approval certification and the above-mentioned contents relevant to the above-mentioned contents, The step which takes amendment actuation when the dependability and integrity of contents with a signature are checked at least using approval certification and misgiving is in any of dependability and integrity they are, The step which controls the operating system of the above-mentioned computer system to guarantee that use of contents with a signature does not exceed the requirements for a resource, and approval certification, How to guarantee the insurance of use of the contents with a signature in the above-mentioned computer system characterized by ****(ing).
(15) The approach of the above-mentioned (14) publication characterized by having further the step registered into a provider by the communication channel, without extracting registration information from a signature and interfering in contents with a signature further at a user.
(16) The approach of the above-mentioned (14) publication characterized by having further the step which controls the above-mentioned operating system to guarantee that extract license conditions from a signature and contents with a signature are in agreement with license conditions.
(17) the above -- computer system -- memory -- inside -- a user -- approval -- certification -- and -- a signature -- entering -- the contents -- a function -- between -- correspondence -- being shown -- a table -- containing -- DS -- forming -- a step -- the above -- correspondence -- following -- a user -- a signature -- entering -- the contents -- using it -- a case -- this -- use -- strengthening -- a step -- further -- having -- things -- the description -- ** -- carrying out -- the above -- (-- 14 --) -- a publication -- an approach .
(18) The approach of the above-mentioned (14) publication characterized by having further the step which operates the above-mentioned process compulsorily so that it may be in agreement with the step and the requirements for a resource which pursue the process generated from contents with a signature, and approval certification.
(19) The contents with a signature are the approaches of the above-mentioned (14) publication characterized by having at least one of an application program and documents.
(20) How to control use of the contents in the above-mentioned computer system characterized by to have the step which imports into computer system contents including the license conditions which can read a computer, the step which extract the license conditions which can read a computer from the contents which imported, and the step which control actuation of the above-mentioned computer system to guarantee that use of contents with a signature is in agreement with license conditions.
(21) The approach of the above-mentioned (20) publication characterized by having further the step automatically registered into a provider by the communication channel, without extracting registration information from a signature and interfering in contents with a signature further at a user.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] Drawing 1 is the epitome Fig. of the contents distribution device by the principle of this invention.

[Drawing 2] Drawing 2 shows the source and repeating installation in a contents distribution system.

[Drawing 3] Drawing 3 shows how repeating installation adds a signature to the contents under distribution according to the example of this invention with a manufacturer/author.

[Drawing 4] Drawing 4 shows the module contained when processing contents with a signature within a user's machine according to the example of this invention.

[Drawing 5] Drawing 5 shows the access information table which the strengthening module of drawing 4 uses.

[Drawing 6] Drawing 6 shows the relation between the capacity of the various entities of an insurance use system for the contents of drawing 4 .

[Drawing 7] Drawing 7 shows the relation between the privileges granted to a user who is different about the contents with a signature of the system of drawing 4 .

[Drawing 8] Drawing 8 shows the example of this invention in case contents with a signature are Java applets.

[Drawing 9] Drawing 9 shows action which the contents insurance use system of drawing 4 takes, when contents with a signature are received.

[Drawing 10] Drawing 10 shows how the strengthening module of drawing 4 strengthens security.

[Description of Notations]

1, 20, 30 User

2 Contents Insurance Use System

3 Operating System

4 11 Machine of a client

5 Contents Distribution Device

6, 23, 24, 25 Contents with a signature

7 List of Approval Certification

8 Requirements for Resource

10 Registration Information

12, 13, 14 Machine for junction

15, 16, 17 Machine of a manufacturer/author

21 Repeating Installation

22 Manufacturer/Author

32 Provider of Contents with Signature

33 Contents Import Device

34 Extractor

35 Analysis Module
36 Contents Interpretation Equipment
37 Strengthening Module
40 Access Information Table
42 Limit of Resource
43 Consumed Resource
44 Required Resource
50 Privilege of Operating System
51 User's Privilege
52 Privilege of Contents Insurance Use System
53 Privilege of Contents with Signature
54 Privilege of Generated Contents
60 User's Installed Privilege
61 User's 1 Privilege
62 User's 2 Privilege
63 User's 3 Privilege
